UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/538,517	03/29/2000	Jun Maruo	SONY-50N3505	6696

7590 05/28/2004	**EXAMINER**
Wagner Murabito & Hao LLP	ARANI, TAGHI T
Two North Market Street	

	ART UNIT	PAPER NUMBER
Third Floor		
San Jose, CA 95113	2131	9

DATE MAILED: 05/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _17 March 2004_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-44_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-44_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claims 1-44 were pending for examination.

Claims 1, 13, 25 and 34 are amended.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is riot identically disclosed or described as set forth in
section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
such that the subject matter as a whole would have been obvious at the time the invention was made to a person
having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the

claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various

claims was commonly owned at the time any inventions covered therein were made absent

any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to

point out the inventor and invention dates of each claim that was not commonly owned at the

time a later invention ways made in order for the examiner to consider the applicability of 35

U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-8, 11-13, 15-16, 18-22, 25-26, 28-31, 33-40, and 43-44 rejected under 35

U.S.C. 103(a) as being unpatentable over prior art of record (Summers et al. and Hendricks

et al.)

Referring to (Amended) claims 1, 13, 25, and 34, Summers et al. teach a transceiver

system for receiving content contained in a secure digital broadcast signal, comprising-

• A first encryption unit coupled to the first component, and for encrypting the data

stream for transmission to generate an encrypted data stream [see figure 4, CP1];

- A second encryption unit coupled to the second component and for decrypting the
  encrypted data stream received from the first component [see figure 4, CP2];

- A bi-directional digital bus coupled to the first encryption unit and the second
  encryption unit [see figure 4, BUS 47 and column 3, lines 59-60]; and

- A third component coupled to the bus for arbitration such that content from the
  data stream is securely transferred across the bus <u>and without exposing an</u>

  <u>unencrypted data stream</u> [see figure 4, KP 46, <u>see also col. 5, lines 1-13, 30-47</u>],

  emphasis added reflecting the added limitation.

  Summers et al. do not teach a transceiver system for receiving content

  contained in a secure digital broadcast signal, comprising;

- A first component for generating a data stream;

- A second component for generating a video signal for a display device;

  However, Hendricks et al. disclose a transceiver system for receiving

  content contained in a secure digital broadcast signal, comprising;

- A first component for generating a data stream [see figure 4, DEMOD 606 and

  column 35, line 41];

- A second component for generating a video signal for a display device [see

  figure 4, NTSC ENCODE 62.5;

  It would have been obvious to one of ordinary skill in the art at the time the

  invention was made to apply Hendricks et al.'s teachings of a first component for

  generating a data stream and a second component for generating a video display to

  the system/method of Summers et al., such that Summers et al's system generate a

data stream to be encrypted and then decrypted at the second component to generate

a video signal for display. One of ordinary skill in the art would have been

motivated to modify Summers et al.'s system as such in order to enable the

generated data stream to be secure at all times and not expose the data in non-

encrypted format.

Referring to claims 2 and 26, Summers et al. as modified teach the system/method

of claims 1 and 25 respectively, wherein the transceiver is a set-top box [see figure 5a of

Hendricks et al.].

Referring to claims 3, 15, 18, 28, and 35, Summers et al. as modified teach the

system/method of claims 1, 13, 25, and 34 respectively, wherein the first component is an

audio video decode block for decoding the data stream from a digital broadcast signal [see

figure 4, DEMOD 606 and column 35, line 41].

Referring to claims 4, 16, 29, and 36, Summers et al. as modified teach the

system/method of claims 1, 13, 25, and 34 respectively, wherein the second component is a

graphics block for generating the video signal from the data stream received from the first

component [see figure 4, NTSC ENCODER 625 of Hendricks et al.].

Referring to claims 5, 19, 30, and 37, Summers et al. as modified teach the

system/method of claims 1, 13, 25, and 34 respectively, wherein the third component a CPU

(central processing unit) block [INFOSEC Controller] coupled to the bus for managing an

encryption process of the first encryption unit and the second encryption unit [see column 4,

lines 65 - 67].

Referring to claims 6, 20, 31, and 38, Summers et al. as modified teach the

system/method of claims 5, 19, 30, and 34 respectively, wherein the encryption process is

key-based encryption process and the CPU block manages the distribution of keys to the first

encryption unit and the second encryption unit [see column 4, lines 65-67 of Summers et al.].

Referring to claims 7, 21, and 39, Summers et al. as modified teach the

system/method of claims 5, 19, and 34 respectively, further comprising an arbiter

coupled to the CPU block for arbitration of the bus [see figure 4, SECURE BUS

ARBITER 40 of Summers et al.].

Referring to claims 11 and 43, Summers et al. as modified teach the system/method of

claims 1 and 34 respectively, further comprising a front end block coupled to the bus for

receiving the digital broadcast signal and generating the data stream therefrom, the first

component coupled to receive the data stream from the front end block via the bus [see

figure 4, **TUNER** 603 of Hendricks et al.].

Referring to claims 12, 33, and 44, Summers et al. as modified teach the

system/method of claims 1, 25, and 34 respectively, wherein the data stream is

substantially compliant with a version of the MPEG (Moving Pictures Experts Group)

format [see column 8, line 24].

Claims 8, 22, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Summers et al. and Hendricks et al., and further in view of Computer Architecture and

Organization to John P. Hayes.

Referring to claims 8, 22, and 40, Summers et al. as modified teach all limitations of

the claims except do not explicitly recite the system/method of claims 1, 19, and 34

respectively, wherein the first component, second component, and third component include

respective identification registers for identifying each component. Nonetheless, it is inherit

in computer architecture, like that taught by Summers et al. and Hendricks et al., that each

component have a register to allow for the CPU to identify the present state of the

component.

However, the examiner herein addresses the possibility that the claimed register

architecture is not inherit in Summers et al. as modified. So, for argument's sake, Summers

et al. as modified is silent as to the provision of registers in the first, second, and third

components.

Hayes does disclose an the system/method of claims 1, 19, and 34 respectively,

wherein the first component, second component, and third component include respective

identification registers for identifying each component [see page 139, Circuit

specification, second paragraph],,

Hence, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to apply Hayes' teachings such that each component of Summers et

al. and Hendricks et al.'s system have a register therein. One of ordinary skill in the art

would have been motivated to modify Summers et al. and Hendricks et al.'s system as

such in order to allow for the CPU to identify the present state of the component.

Claims 9-10, 14, 23-24, 27, 32, and 41-42 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Summers et al. and Hendricks et al., and further in view of U.S.

Patent No. 5,805,706 to Davis (prior art of record).

Referring to claims 9, 23, 32, and 41, Summers et al. and Hendricks et al. do not

explicitly teach the system/method of claims 1, 19, 25, and 34 respectively, wherein said

data stream is encrypted using an encryption process substantially compliant with DES

ECB (Data Encryption Standard Electronic Code Book).

However, Davis does disclose the system/method of claims 1, 19, 25, and 34

respectively, wherein said data stream is encrypted using an encryption process

substantially compliant with DES EC13 (Data Encryption Standard Electronic Code

Book) [see column 3, line 16].

It would have been obvious to one of ordinary skill in the art at the time the inventions

was made to apply Davis' teachings of a DES compliant encryption process, such that the

encryption units of Summers et al. and Hendricks et al. perform DES encryption. One of

ordinary skill in the art would have been motivated to modify Summers et al and

Hendricks et al.'s system as such in order to make it compliant with industry standards

and thus easing the integration of the subsystem into other systems.

Referring to claims 10, 24, 27 and 42, Summers et al. and Hendricks et al. do not

teach the system/method of claims 1, 19, 25, and 34 respectively, wherein the bus

is a PCI (Peripheral Component Interconnect) compliant bus and each encryption unit

performs encryption and decryption.

However, Davis does disclose the system/method of claims 1, 19, 25, and 34

respectively, wherein the bus is a PCI (Peripheral Component Interconnect) compliant bus

and each encryption unit performs encryption and decryption [see column 3, line 36 and

column 4, lines 57-58].

It would have been obvious to one of ordinary skill in the art at the time the inventions was made to apply Davis' teachings of a PCI bus and each encryption unit performing encryption and decryption, such that the encryption units of Summers et al. and Hendricks et al. perform encryption and decryption. One of ordinary skill in the art would have been motivated to modify Summers et al and Hendricks et al.'s system as such to enable the cryptographic unit to decrypt or encrypt data that is sent and received via the PCI bus (bi-directional).

Referring to claim 14, Summers et al. and Hendricks et al. do not teach the architecture of claim 13 wherein the first component and the first encryption unit are built into a first integrated circuit device and the second component and the second encryption unit are built into a second integrated circuit device.

However, Davis does disclose the architecture of claim 13 wherein the first component and the first encryption unit are built into a first integrated circuit device and the second component and the second encryption unit are built into a second integrated circuit device [see column 4, lines 19-24].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Davis' teachings such that the encryption unit and first and second components of Summers et al. and Hendricks et al. are built into integrated circuit devices. One of ordinary skill in the art would have been motivated to modify Summers et al. and Hendricks et al.'s system as such in order to add an extra level of secure for the plain text or key information.

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Summers et al. and Hendricks et al., and further in view of U.S. Patent No. 5,872,846 to Ichikawa (prior art of record).

Referring to claim 17, Summers et al. and Hendricks et al. do not teach the architecture of claim 13 wherein the first component is a conditional access block for descrambling the digital broadcast signal.

However, Ichikawa does disclose the architecture of claim 13 wherein the first component is a conditional access block for descrambling the digital broadcast signal [see figure 3, First-Level Decoder 332, Key 308].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Ichikawa's teachings of a conditional access block such that the first component of Summers et al. and Hendricks et al. is a conditional access block. One of ordinary skill in the art would have been motivated to modify Summers et al. and Hendricks et al.'s system as such in order to allow only the authorized subscriber to obtain the program.

Response to Amendment

Applicant's arguments filed 3/17/2004 regarding the rejection of the claims under 35 U.S.C. 103() have been fully considered but they are not persuasive. Applicant's attempt to distinguish the claims from prior art is based on noting the lack of a teaching of " the generation of data stream, the encryption of data stream, and the secure transfer of the data stream across a bus and among components and without exposing an unencrypted data stream ", page 15 third paragraph of the Applicant's REMARKS. This feature was found to

be taught by Summers SBA. That is, the SBA of Summers' invention works under the

control of a trusted kernel and operating system which prevents other untrusted processors or

devices from compromising classified or sensitive data, col. 5, lines 30-47 and that Summers'

invention provides isolation of the data over the bus from all other computer elements not

associated with the data class throughout its processing and transfer through the system, col.

5, lines 7-13.

The Applicant argues that " Summers doe not appear to show any special mechanism or

procedures for preventing exposure of an unencrypted data stream", page 16, third paragraph

of the REMARKS.

The Examiner disagrees. In fact, Summers' apparatus is provided to handle classes of

data in computer systems that must not be permitted to intermingle due to their security

classifications and critically of their data contents and that Summers' SBA with a controller

provide a way to isolate data without modification of the computer back plane, see abstract.

Furthermore, Summer discloses that arbiter function control in the motherboard

determines what cards are allowed access to the computer data bus to perform secret,

classified or non-secret sensitive data handling, col. 1, lines 37-44.

Action is Final

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set

forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until

after the end of the THREE-MONTH shortened statutory period, then the shortened statutory

period will expire on the date the advisory action is mailed, and any extension fee pursuant to

37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from examiner

should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner

can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the

organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100